REMARKS

INTRODUCTION

Claims 1-23 were previously pending and under consideration.

Claims 24-26 are added herein.

Therefore, claims 1-26 are now pending and under consideration.

Claims 1-23 are rejected.

Claims 1, 4, 6-14 and 16-23 are amended herein.

No new matter is being presented, and approval and entry are respectfully requested.

CHANGES TO THE SPECIFICATION

The specification has been reviewed in response to this Office Action. Changes have been made to the specification only to place it in preferred and better U.S. form for issuance and to resolve the Examiner's objections raised in the Office Action. No new matter has been added.

REJECTIONS UNDER 35 USC § 112, SECOND PARAGRAPH

In the Office Action, at page 2, claims 4 and 9 were rejected under 35 U.S.C. § 112, second paragraph, for the reasons set forth therein. The formalities have been corrected. Withdrawal of the rejection is respectfully requested.

REJECTIONS UNDER 35 USC § 103

In the Office Action, at pages 3-5, claims 1, 2, 4-6 and 9-11 were rejected under 35 U.S.C. § 103 as being unpatentable over Davis in view of Bellare. Claims 3, 8 and 12-23 were rejected under 35 U.S.C. § 103 as being unpatentable over Davis in view of Bellare and Rogaway. These rejections are traversed and reconsideration is requested.

AUTHENTICATORS OF DAVIS NOT LINKED TO AND SEPERATED FROM THE INFORMATION USED TO CREATE THE AUTHENTICATORS

Claim 1, for example, recites that authenticators are created for "each of the divided data from the information to be signed". The authenticators are then linked to "the respective divided data of the information from which the authenticators were created". In other words, any given authenticator is matched with a respective divided data. See also claims 6, 11, 12, 13, 16, 17, 20, and 21.

These features offer various advantages, for example a would-be attacker would need to know additional information such as which hash function corresponds to which division of data and its authenticator, thus multiplying the difficulty of breaking or spoofing the overall signature scheme. Rather than linking each authenticator to its data/section, Davis' Hash table 137 (a combination of separate hashes of sections of coefficients) simply concatenates the various hashes of, for example, sections A-D ("digests ... are concatenated together", col, 5, lines 35-37). Concatenation in Davis is not the same as linking hashes/authenticators to the data from which the hashes/authenticators were generated. Furthermore, there is no need in Davis to link the individual authenticators to their respective sections because (1), as discussed below, the hash functions of Davis are the same for a given image signature, and (2) the sections are divided in a predetermined manner on variable-size sections (also discussed below). For example, exactly 4 variable-size sections are used regardless of the size of the compressed image data.

Further to the feature discussed above, claim 1 for example recites the certifier/receiver "separating the information and the linked plurality of authenticators from the data received from said signing station". Not only does Davis not link authenticators to sections, Davis does not separate them. In Davis, a convention or predetermined number of sections is used at any given time.

Bellare was not cited as providing the features discussed above. Other independent claims recite features similar to those discussed above. Withdrawal of the rejection is respectfully requested.

DAVIS DISCLOSES ONE HASH FUNCTION RATHER THAN PLURAL DIFFERENT HASH FUNCTIONS

Claim 1, for example, recites "creating a plurality of authenticators by applying a different one-way function to each of the divided data divided from the information to be signed". In other words, for divided data of information to be signed, plural one-way functions are used. In contrast, Davis discusses only one hash function; "[e]ach set of coefficients is run through **a** hashing function" (col. 5, lines 21-23); "**a** hash function" (col. 3, lines 35-37). Although Davis mentions different hash functions at col. 5, lines 23-28, it is referring to different embodiments, each using a particular different function as the same hash function for hashing each section (this is similar to the suggestion to used different encryption algorithms such as RSA and DES; only one such algorithm is used in any particular embodiment.

At best, Davis is ambiguous about whether the divided sections have different hash functions in one embodiment. The prior art does not disclose or suggest one embodiment signing divided information (e.g. document, image, etc.) using plural different functions. Only the present application provides a reason why plural different functions would be beneficial. Absent some suggestion to the contrary, the software design principle of simplicity and code reuse suggests that Davis uses only one hash function to hash the different sections. Put another way, in general, absent some specific reason, algorithms do not use different functions to perform the same purpose. For example, absent some reason to the contrary, a quicksort algorithm would use the same comparison function for each sort.

The other prior art references were not cited as providing this feature.

Withdrawal of the rejection is further respectfully requested.

PRIOR ART DOES NOT DISCLOSE DIVIDING INTO PRESPECIFIED LENGTH SECTIONS/DIVISIONS OF DATA

The sections of Davis are image data sections of variable length, each having coefficients representing a different level of detail of an image. Therefore, the hash function of Davis is applied to calculated coefficients, rather than divided data of information to be signed. If Davis were analogous, it would divide the image data into divisions of data of the image itself (information to be signed), rather than sets of coefficients. This difference also highlights how

Davis is applicable only with lossy compression data rather than the general purpose applicability of the presently claimed invention.

Similarly, the hashes of the sections in Davis are sent from the sender to the receiver as a single concatenated hash sequence 137. Thus they do not need to be "separated from the data received ...".

Withdrawal of the rejection is further respectfully requested.

DEPENDENT CLAIMS

The dependent claims are deemed patentable due at least to their dependence from allowable independent claims. These claims are also patentable due to their recitation of independently distinguishing features. For example, claim 2 recites "truncating the authenticators created by said first authenticator creating unit to the information". This feature is not taught or suggested by the prior art. Withdrawal of the rejection of the dependent claims is respectfully requested.

NEW CLAIMS

New claims 24-26 have been added to clarify an aspect of the present invention in which non-image data is operated on. The prior art discusses only lossy image compression data.

STEP LANGUAGE REMOVED

To clarify that §112, paragraph six is inapplicable to the present claims, "step" language has been removed. This change to the claims does not narrow the claims.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 8 March 2004

By: James Strom
James T. Strom
Registration No. 48,702

1201 New York Avenue, NW
Suite 700
Washington, D.C. 20001
(202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE UNDER 37 CFR 1.8(a)
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on March 8, 20 04
STAAS & HALSEY
By: Darlene Anderson
Date: March 8, 2004